QUALYS SECURITY CONFERENCE 2020

Moving Security up the Stack
Web Application and API Security

Dave Ferguson
Director of Product Management, Qualys, Inc.

Agenda

Recent trends in Application Security

Web Application Scanning (WAS)

Qualys Periscope

Building Securing APIs

Trends in Application Security

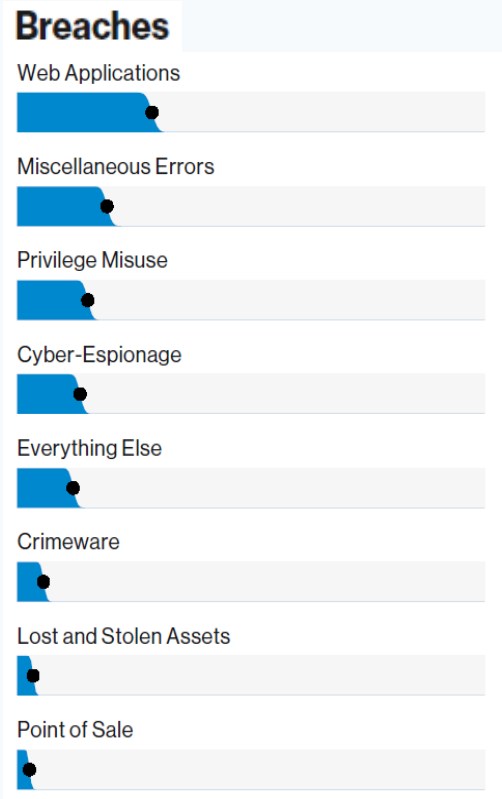
Web app breaches continue

E-commerce sites targeted

API attacks

Trends in AppSec testing

- Shifting left
- Coverage
- Automation



Source: 2019 Verizon DBIR

Qualys.

Web Application Scanning

WAS Overview

Detects application-layer vulnerabilities in web apps & APIs

Browser engine

Automated crawling

Play back of Selenium scripts

API to integrate with other systems

Unique integration with Qualys WAF

Mature product

Qualys.

2019 Highlights

WAS Jenkins plugin v2

Updated Qualys Browser Recorder

TLS 1.3

Full HTTP requests

Enhanced crawling

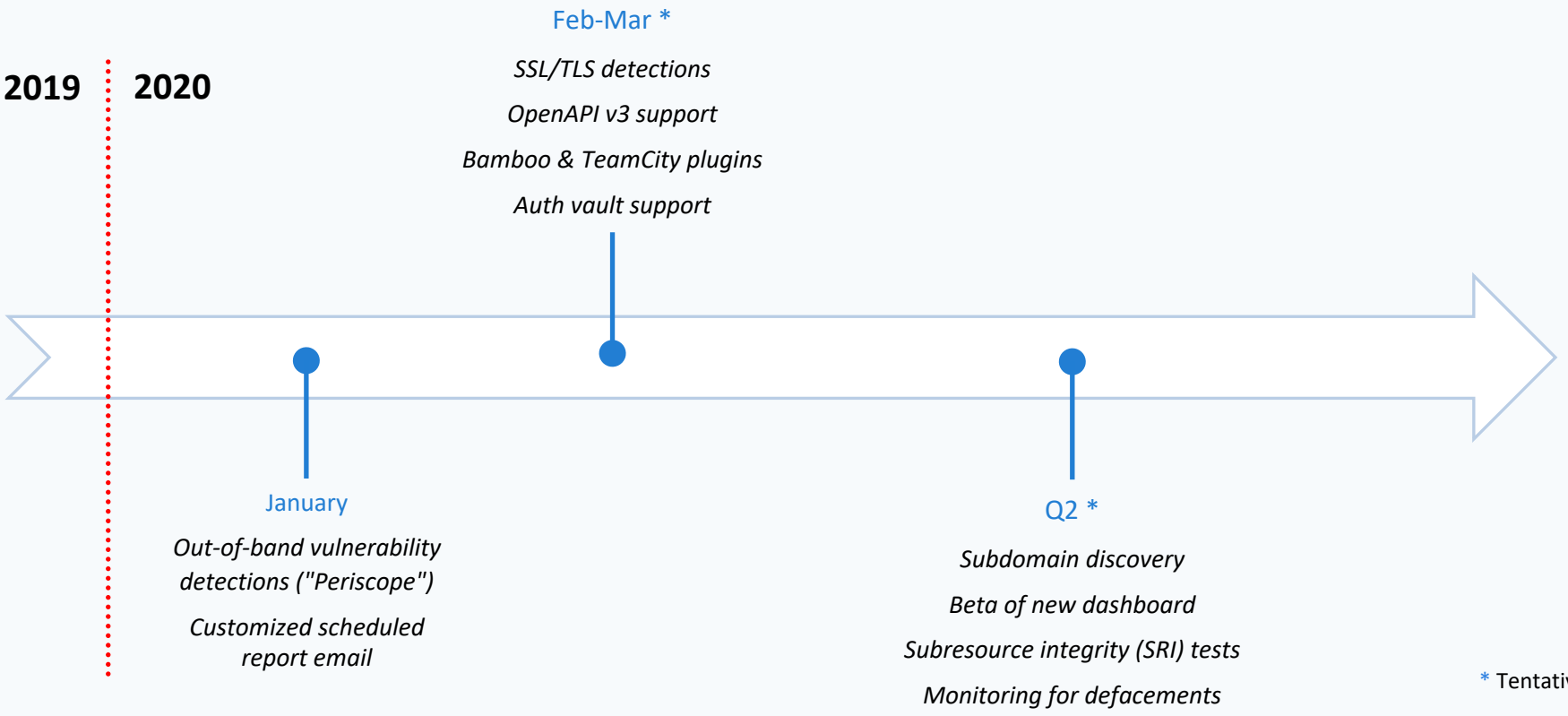
Postman Collections

WAS Burp extension v2

Editable QID severity

Qualys.

WAS Roadmap



* Tentative

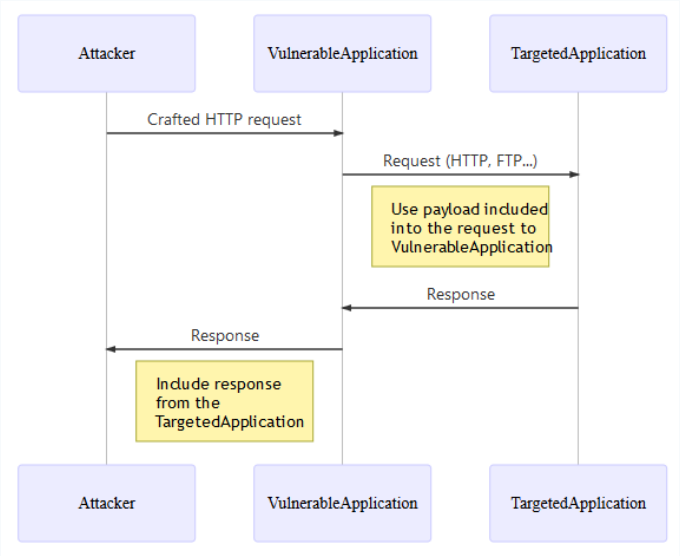
Qualys.

Out-of-Band Vulnerabilities

Some issues can't be detected by traditional request-response

- SSRF
- SMTP header injection
- Blind XXE injection

Detecting these vulnerabilities requires a different approach



Source: OWASP

Qualys.

Introducing Periscope

Detection mechanism for out-of-band web app vulnerabilities

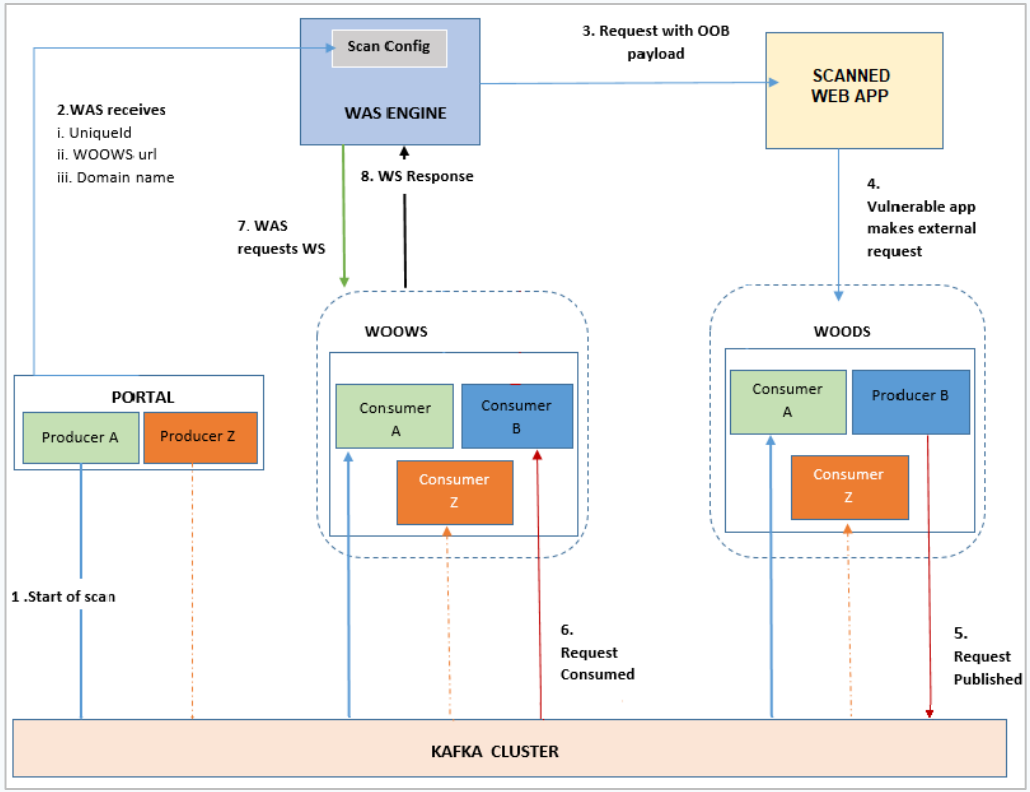
Scanner sends a test; POST request body is:

p1=joe&p2=smith&p3=http%3A%2F%2Fe528efddaa51766cb86afb19f22de54b6da1093c.1454156_35626.2086421852.ssrf01.ssrf.qualysperiscope.com

The web app tries to resolve this FQDN:

e528efddaa51766cb86afb19f22de54b6da1093c.1454156_35626.2086421852.ssrf01.ssrf.qualysperiscope.com

Qualys Periscope



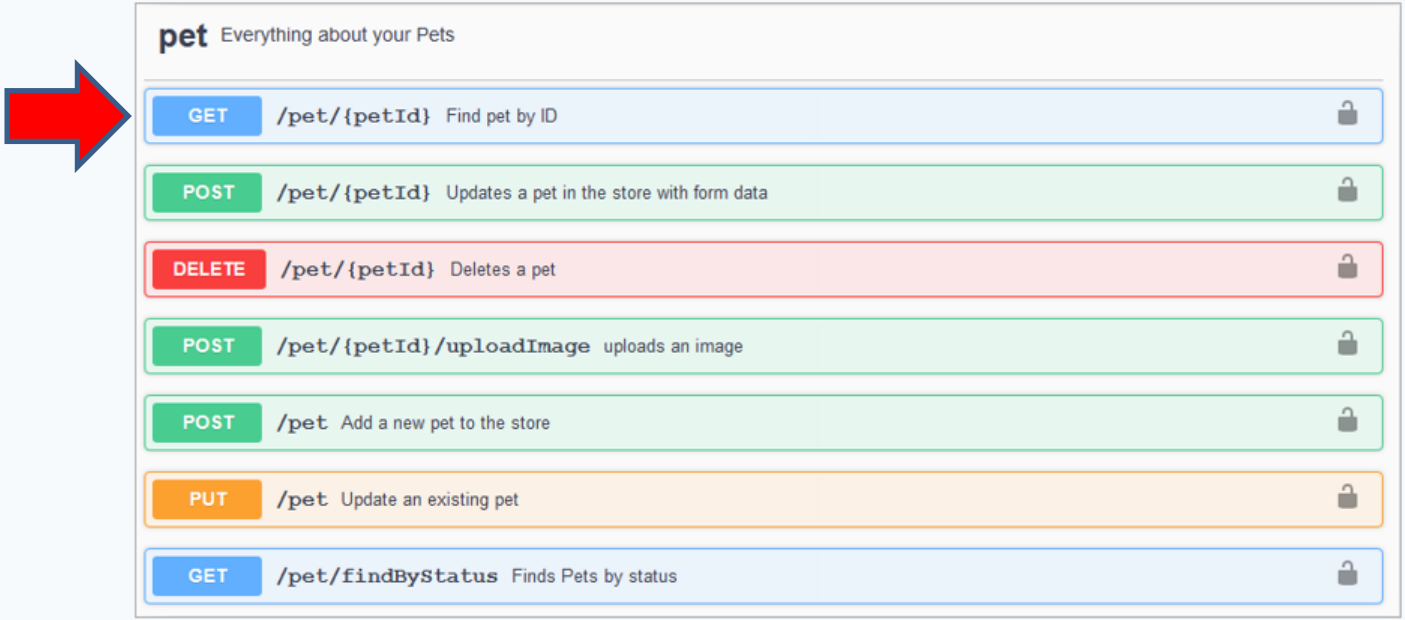
Qualys.

Building Secure APIs

OWASP API Security Top 10

1	Broken Object Level Authorization (BOLA)
2	Broken User Authentication
3	Excessive Data Exposure
4	Lack of Resources & Rate Limiting
5	Broken Function Level Authorization
6	Mass Assignment
7	Security Misconfiguration
8	Injection
9	Improper Assets Management
10	Insufficient Logging & Monitoring

Example API – Pet Store



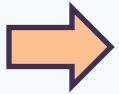
Relevant portion of the Swagger File

```
{
  "swagger": "2.0",
  "info": {
    "version": "1.0",
    "title": "Petstore",
   },
  "host": "api.petstore.com",
  "basePath": "/v1",
  "schemes": [
    "http", "https"
  ],
  "paths": {
    "/pet/{petId}": {
      "get": {
        "summary": "Get info for a specific pet",
        "operationId": "showPetById",
        "parameters": [
          {
            "name": "petId",
            "in": "path",
            "required": true,
            "description": "The ID of the pet to retrieve",
            "type": "integer"
          }
        ],
        "responses": {
          "200": {
            "description": "Expected successful response",
            "schema": {
              "$ref": "#/definitions/Pet"
            }
   ...snip...
```

How Does this Help with Security?

We can leverage the Swagger spec to harden the API endpoints in a declarative way

```
"paths": {
    "/pet/{petId}": {
      "get": {
        "summary": "Get info for a specific pet",
        "operationId": "showPetById",
        "parameters": [
          {
            "name": "petId",
            "in": "path",
            "required": true,
            "description": "The ID of the pet",
            "type": "integer"
          }
        ],
```



```
"paths": {
    "/pet/{petId}": {
      "get": {
        "summary": "Get info for a specific pet",
        "operationId": "showPetById",
        "parameters": [
          {
            "name": "petId",
            "in": "path",
            "required": true,
            "description": "The ID of the pet",
            "type": "integer",
            "minimum": 1,
            "maximum": 999999
          }
        ],
```

Qualys.

Capabilities Coming to Qualys API Security

Static Assessment of Swagger/OpenAPI file

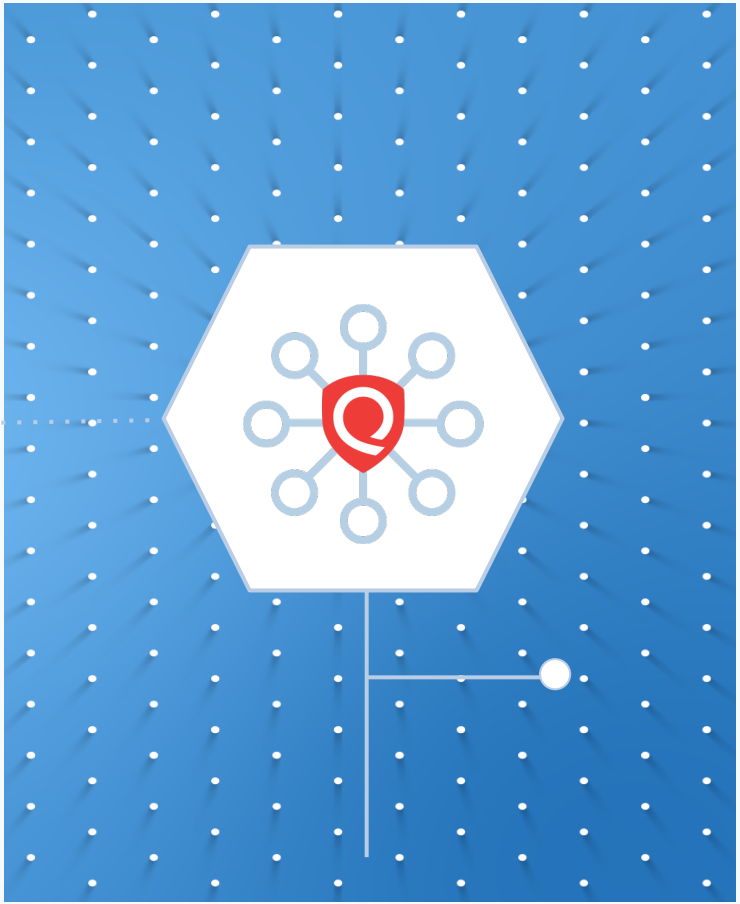
Get recommended changes to harden your API

Conformance Scan to check the API's actual behavior

Test the API endpoints for behavior that violates the Swagger file

Vulnerability Scan to check the API for security flaws

Current feature in Qualys Web Application Scanning (WAS)



Qualys.

Thank You

Dave Ferguson
dferguson@qualys.com

QUALYS SECURITY CONFERENCE 2020

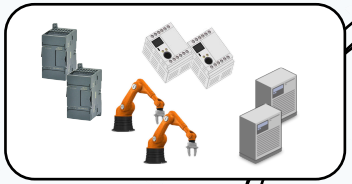
Industry Control Systems
Making ICS/OT a Part of Overall Vulnerability Management Program

Dharmesh Ghelani
Principal Product Manager, Qualys, Inc.

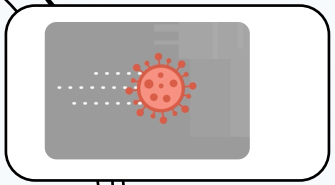
Industrial Control Systems

Are becoming internet-aware

1. ICS SYSTEMS



2. ARE GETTING TARGETED

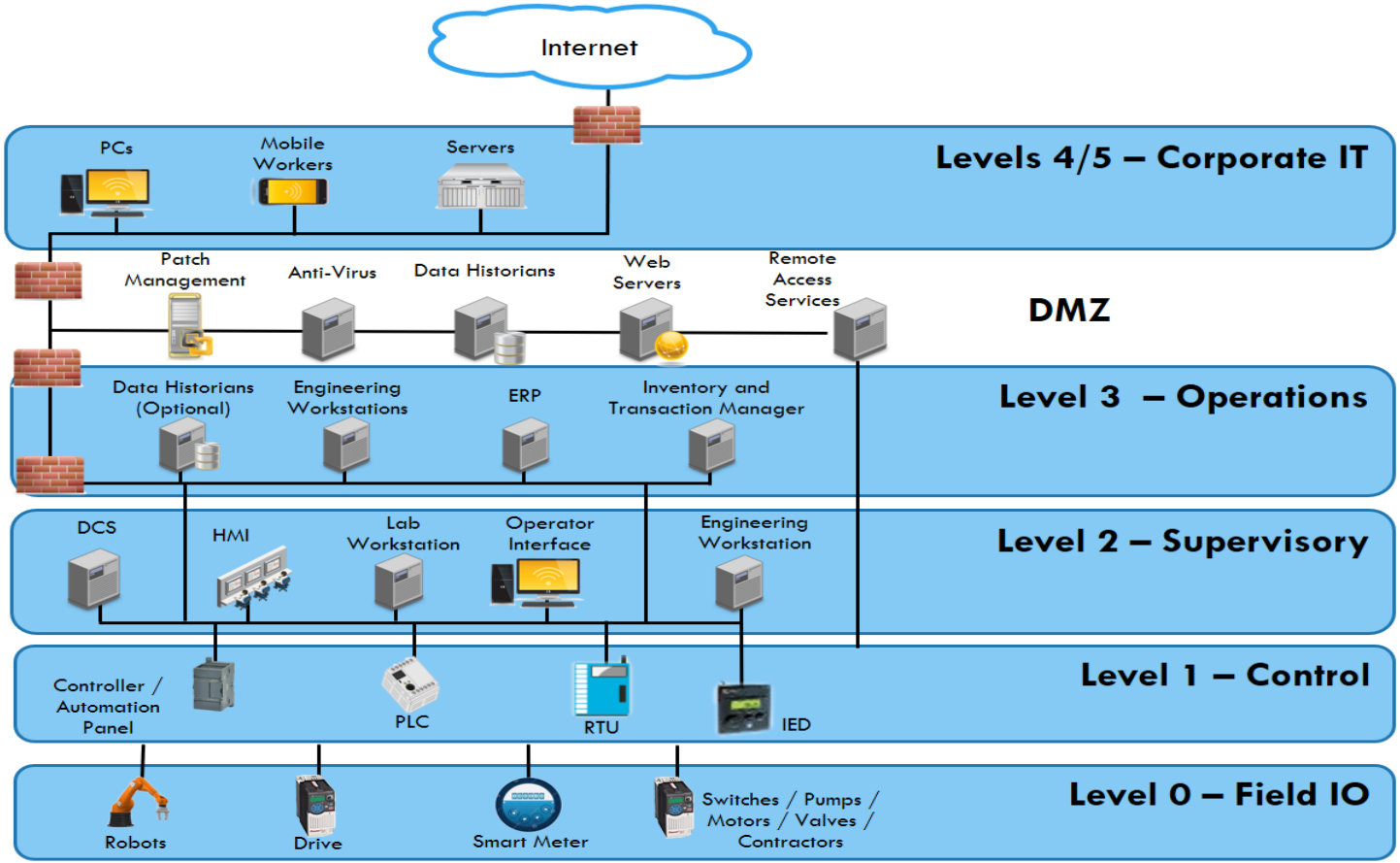


Qualys.
Industrial Control Security

3. ATTACKS CAN BE PREVENTED

Qualys.

Typical Industrial Control Networks



Qualys.

Qualys Industrial Control Security v1.0

Use cases

Visibility
- Inventory
- Network Topology

Vulnerability Management

Technology

Passive Sensor

- ✓ Mirror Port
- ✓ 100% Passive

Qualys Scanner

- ✓ Safe Active Probes
- ✓ ICS Scan Types
- ✓ Granular Controls

Cloud Agent

- ✓ SCADA Serves / ERP Systems / HMI Servers
- ✓ All Industrial PCs

Vulnerability Signatures

Rockwell Automation · Allen-Bradley · Rockwell Software · ABB · SIEMENS · GE · YOKOGAWA · Schneider Electric · MITSUBISHI ELECTRIC · KUKA · Honeywell · Johnson Controls

Demo

High Level Roadmap

Design Partnership Q1 '20 → **V 1.0 Beta** → **ICS V 1.0**

v1.0 Protocols…

➢ **Most Prevalent**
- S7 Comm / Plus
- Profinet
- Ethernet IP
- BACnet
- Modbus TCP
- OPC Suite
- DNP3
- MSS / GOOSE
- IEC 104
- CC Link IE
- MQTT
- Omron Fins
- EtherCAT
- Nigara Fox
- Ethernet Powerlink

➢ **Design Partnership**
- *MelsecNet*
- *PCCC*
- …

➢ **IT Protocols**
- CDP
- LLDP
- TFTP / FTP
- HTTP / HTTPS
- Telnet
- SMB/CIFS

v1.0 Major Vendors…

➢ **Most Prevalent**
- Siemens
- Rockwell Automation
- Schneider Electric
- ABB
- GE
- Kuka
- Johnson Control

➢ **Design Partnership**
- *Mitsubishi Electric*
- …

Qualys.

Qualys Industrial Control Security Roadmap

Compliance

Threat Detection

Process Integrity

Zones & Conduits Access Controls

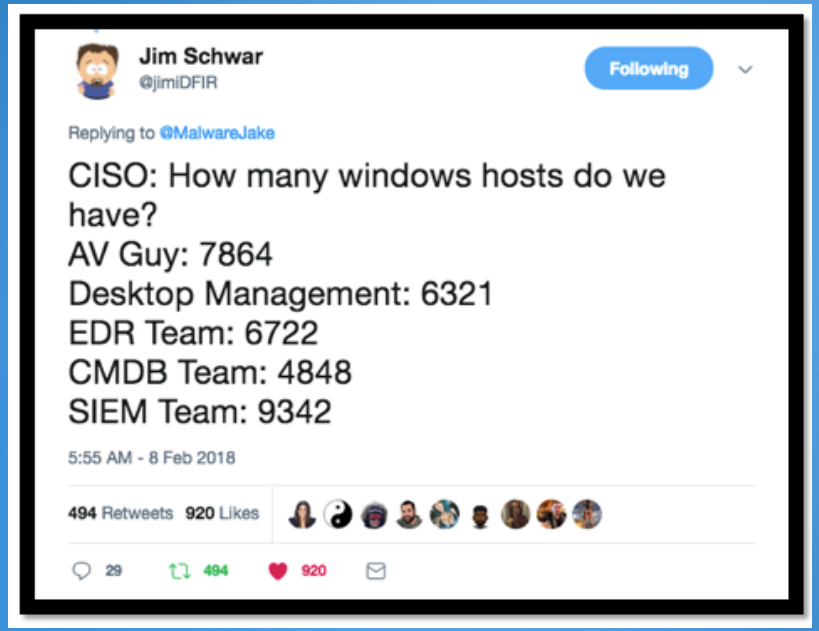
Thank You

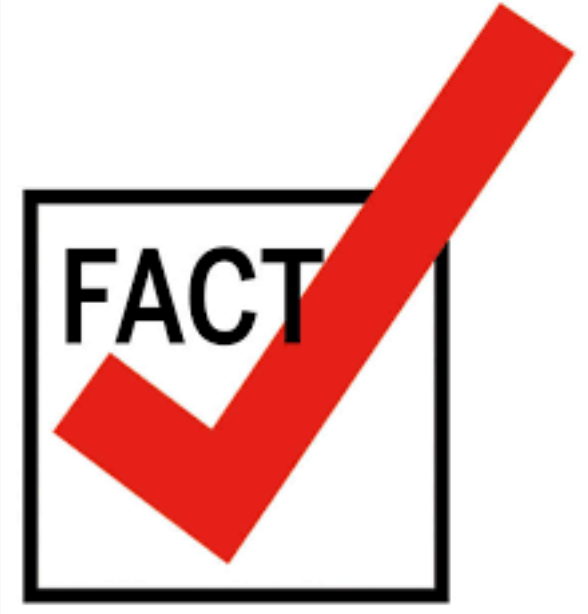
Dharmesh Ghelani
dghelani@qualys.com

Global IT Asset Inventory

A new Prescription for Security

Pablo Quiroga
Director, Product Management, Qualys, Inc.


Jim Schwar
@jimiDFIR
Following
Replying to @MalwareJake
CISO: How many windows hosts do we have?
AV Guy: 7864
Desktop Management: 6321
EDR Team: 6722
CMDB Team: 4848
SIEM Team: 9342
5:55 AM - 8 Feb 2018
494 Retweets 920 Likes
29
494
920



You Can’t Secure What You Don’t See or Know

Global Hybrid-IT Environment

On-Premise?

Cloud, …Containers?

Endpoints, Remote Workforce?

Mobility?

IoT, IIoT, OT?

I need visibility across everything!

Cloud Agent

Passive Sensor

Network Scanner

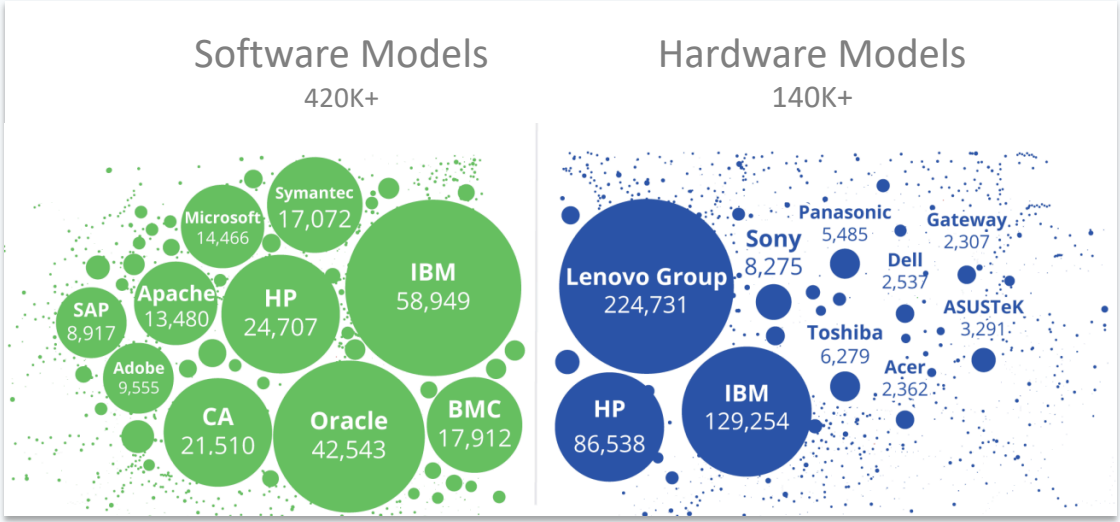
Connectors
(AWS, Azure, GCP)

	Operating Systems	Hardware	Software
Raw Data	Base OS Runtime AIX: 06.01.0009.0300 EE	Dell, Inc. R510	mysql-community-server 5.6.35-2.el7.x86_64

Other Tools

	Operating Systems	Hardware	Software
Raw Data	Base OS Runtime AIX: 06.01.0009.0300 EE	Dell, Inc. R510	mysql-community-server 5.6.35-2.el7.x86_64
Category	UNIX > Server	Computers > Server	Databases > RDBMS
Manufacturer	IBM	Dell	Sun Microsystems
Owner	IBM	Dell	Oracle
Product	AIX	PowerEdge	MySQL Server
Market Version / Model	6	R510	5
Edition	Enterprise	-	Community
Version	6.1	-	5.6
Update	TL9 SP3	-	35-2.el6
Architecture	64-Bit	-	64-Bit
Lifecycle Stage	EOL/EOS	OBS	EOL
End-of-Life	30-Apr-2015	1-Sep-2012	28-Feb-2018
End-of-Support	30-Apr-2017	1-Sep-2012	28-Feb-2021
Support Stage	Unsupported	Obsolete	Extended Support
License Type	Commercial	-	Open Source (GPL-2.0)

Continuous IT Asset Intelligence as a Service



Qualys.

DEMO

Thank You

Pablo Quiroga
pquiroga@qualys.com

QSC Paris

Apéritif et animations

17:30 – 20:30

Le Royal Monceau